



PATENT
Attorney Docket No. 09812.0583-00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
Yoshihito ISHIBASHI et al.) Group Art Unit: 2165
Application No.: 09/396,054) Examiner: Neveen ABEL JALIL
Filed: September 15, 1999) Confirmation No.: 6914
For: CONTENT MANAGEMENT)
METHOD, AND CONTENT)
STORAGE SYSTEM)

Mail Stop Appeal Brief--Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

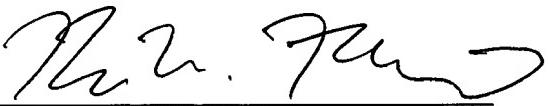
In response to the Notification of Non-Compliant Appeal Brief mailed February 6, 2008, Appellants submit a replacement Section V for the Appeal Brief filed on December 3, 2007.

This Appeal responds to the May 31, 2007, final rejection of claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 under 35 U.S.C. § 103(a).

To the extent any additional extension of time under 37 C.F.R. § 1.136 is required to obtain entry of this response, such extension is hereby respectfully requested. If there are any fees due under 37 C.F.R. §§ 1.16 or 1.17 which are not enclosed herewith, including any fees required for an extension of time under 37 C.F.R. § 1.136, please charge such fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: April 2, 2008
By: 
Reece Nienstadt
Reg. No. 52,072

V. SUMMARY OF CLAIMED SUBJECT MATTER**A. Independent Claim 1**

Independent claim 1 is directed to a content management method for managing content data provided to user equipment. The method includes storing a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key in the user equipment. The first storage key is stored in a key management unit. The encrypted content key and the second storage key are sent to the key management unit. At the key management unit, the encrypted content key is decrypted using the first storage key. The decrypted content key is encrypted using the second storage key. The content key, which is encrypted with the second storage key, is sent to the user equipment. At the user equipment, the encrypted content key is decrypted using the second storage key. Using the decrypted content key, the content data is decrypted.

An exemplary embodiment of this content management method is described in the Specification at, for example, pg. 14, line 8 to pg. 17, line 9. This embodiment is also illustrated in Figure 5 of the Specification.

B. Independent Claim 20

Independent claim 20 is directed to a content management system for managing content data. The system includes a storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key. The first storage key is stored in a key management unit. The system has a sending means for sending the encrypted content key and the second storage key to the key management unit. A first decrypting means in the key

management unit is provided for decrypting the encrypted content key using the first storage key. An encrypting means is provided for encrypting the decrypted content key using the second storage key. A second decrypting means is provided for decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.

An exemplary embodiment of this content management system is described in the Specification at, for example, pg. 14, line 8 to pg. 17, line 9. This embodiment is also illustrated in Figure 5 of the Specification.

The content management system recited in claim 20 comprises the element of “a storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key.” An exemplary embodiment of this “storing means” is described in the Specification at, for example, pg. 15, line 11 to line 21, and pg. 16, line 7 to line 13. This embodiment of the “storing means” is also shown in Figure 5 of the Specification as the “external storage” at reference number 22.

The content management system recited in claim 20 further comprises the means-plus-function element of “a sending means for sending the encrypted content key and the second storage key to a key management unit.” An exemplary embodiment of this “sending means” is described in the Specification at, for example, pg. 15, line 11 to line 21. This embodiment of the “sending means” is also shown in Figure 5 of the Specification as the “receiver” at reference number 14. An exemplary embodiment of the “key management unit” is shown in Figure 5 as the “key management center” at reference number 13.

Claim 20 further recites the means-plus-function element of “a first decrypting means, in the key management unit, for decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit.” An exemplary embodiment of this “first decrypting means” is described in the Specification at pg. 15, line 11 to line 21. This embodiment of the “first decrypting means” is also shown in Figure 5 of the Specification as the “key management center” at reference number 13. An exemplary embodiment of the “key management unit” is also shown in Figure 5 as the “key management center” at reference number 13.

Claim 20 also recites the means-plus-function element of “an encrypting means for encrypting the decrypted content key using the second storage key.” An exemplary embodiment of this “encrypting means” is described in the Specification at, for example, pg. 15, line 11 to line 21. This embodiment of the “encrypting means” is also shown in Figure 5 of the Specification as the “key management center” at reference number 13.

In addition, claim 20 recites the means-plus-function element of “a second decrypting means for decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.” An embodiment of this “second decrypting means” is described in the Specification at, for example, pg. 16, line 7 to line 13. This embodiment of the “second decrypting means” is also shown in Figure 5 of the Specification as the “receiver” at reference number 14.